A Security Architectural Pattern for Risk Management of Industry Control Systems within Critical National Infrastructure

Andy Wood

Department of Computer Science and Informatics,
De Montfort University
The Gateway, Leicester, LE1 9BH, UK
Email: P11250192@my365.dmu.ac.uk

Ying He *

Department of Computer Science and Informatics,
De Montfort University
The Gateway, Leicester, LE1 9BH, UK
Email: ying.he@dmu.ac.uk
* Corresponding author

Leandros A Maglaras

Department of Computer Science and Informatics,
De Montfort University
The Gateway, Leicester, LE1 9BH, UK
Email: leandros.maglaras@dmu.ac.uk

Helge Janicke

Department of Computer Science and Informatics,
De Montfort University
The Gateway, Leicester, LE1 9BH, UK
Email: heljanic@dmu.ac.uk

Abstract:

SCADA and ICS security have been focusing on addressing issues such as vulnerability discovery and intrusion detection within critical national infrastructure. Less attention has been paid to architectural solutions to the cyber security risks from an information assurance perspective. Security controls are not always traced back to the business requirements. This paper presents a holistic end-to-end view of the requirements, medium to high severity risks and proposes a generic security architectural pattern to address them. The architectural pattern is developed based on the Sherwood Applied Business Security Architecture (SABSA) top two layers, contextual and conceptual, which are responsible for understanding the business requirements and development of a concept architecture and strategy. Moreover, this research is motivated by industrial practices and has reflected the recent changes of GCHQ's mission. This research

also contributes to the SCADA/ICS risk assessment by deriving holistic sets of risk management and architectural design requirements for SCADA/ICS.

Keywords: Industry Control Systems; Critical National Infrastructure; Security Architectural Pattern; Risk Management; Business Requirements; SABSA.

Biographical notes:
Mr. Andy Wood is Head of Security Architecture & Design at Capita IT Professional Services. He is also doing a PhD in De Montfort University, UK. His research interests are Industrial Control Systems, Secure Smart Environments looking at vulnerabilities and developing counter measures for Cyber-Physical Systems (CPS), Machine 2 Machine (M2M) and Internet of Things (IoT).

Dr. Ying He is a Lecturer of Computer Science in the School of Computer Science and Informatics at De Montfort University, UK. She obtained her PhD in Computer Science from Glasgow University, UK. Ying's research focuses on security risk management, decision-making, business analytics and human's aspects of security. She also looks at how security management frameworks can be applied in different industries.

Dr. Leandros Maglaras received the B.Sc. degree from Aristotle University of Thessaloniki, Greece in 1998, M.Sc. in Industrial Production and Management from University of Thessaly in 2004 and M.Sc. and PhD degrees in Electrical & Computer Engineering from University of Volos, in 2008 and 2014 respectively. He is currently a visiting Lecturer in the School of Computer Science and Informatics at the De Montfort University, U.K. He is an author of more than 60 papers in scientific magazines and conferences and is a senior member of IEEE. His research interests include wireless sensor networks, Scada systems and vehicular ad hoc networks.

Dr. Helge Janicke is the Head of School of Computer Science and Informatics at De Montfort University, UK. His interests are covering formal verification techniques and their application to Cyber Security, SCADA and Industrial Control System Security as well as aspects of Cyber Warfare. He is working closely with Airbus Group and established DMU's Airbus Group Centre of Excellence in SCADA Cyber Security and Forensics Research in 2013. He is a general chair of the International Symposium on SCADA and Industrial Control Systems Cyber Security Research (ICS-CSR) as well as serving on the editorial board and as reviewer of international journals.

1 Introduction

1.1 Background

Supervisory Control And Data Acquisition (SCADA) and Industrial Control Systems (ICS) have been at the forefront of the news in recent years, in particular, the event at Iranian nuclear enrichment facility in 2010 [1], the Stuxnet malware caused enrichment centrifuges. It provided false healthy status to the control centre computers. According to a 2013 survey [2] of nearly 700 participants conducted by the SANS institute, attack vectors of most concern against SCADA and ICS services include internal threat actors, advanced zero-day malware (i.e. Stuxnet or Flame) and external threats from hacktivists, terrorists or governments. Nearly 70% of responses indicated the threat to be high or severe in nature.

The top three primary drivers in relation to security with SCADA and ICS systems listed are control system service interruption prevention, damage prevention and information leakage prevention. The participants roles include average business user, auditor, IT director and manager, network administrator, security analyst, security manager, and others, among which security analyst accounts for 51%.

In recent years, there has been many studies conducted and papers written covering various aspects of SCADA and ICS security [3, 21, 22, 23, 24, 29, 30, 31, 32]. Studies relating to security risk management include the application of the attack tree [25, 26] and diagrammatic risk modeling approach [27]. Extant work also provides control system security standards, guidelines and best practices providing guidance on security risk management. These include IEC/ISA-62443 [4], the internationally recognised industrial control system security standard, NIST SP 800-82 [5], a cross-industry guidance for establishing secure industrial control systems (ICS), the UK's CPNI [6], a good practice guide for ICS security and the U.S. Department of Homeland Security's [7] guidance on the enhancement of ICS security. NIST SP 800-82 does an excellent job of providing best practice guidance for each of the various aspects of securing ICS/SCADA networks, however, it does not take a holistic business view and allow business requirements to be used to drive the controls. Moreover, there is a lot of information to get through before the reader can start to pull together a viable conceptual solution. There is a need of a generic architectural pattern that develops a target architecture based on a set of documented requirements, threats and risks, which can be adapted to suit. The UK's CPNI is a useful document but does not develop an architecture from the business requirements down. Businesses are in need of seeing that architectures are in support of the business requirements and by showing transparently they are through the use of attribute profiling that makes it transparent to auditing and review.

1.2 Motivation

Fernandez et al. [9] proposed methods to build a secure SCADA system using security patterns. They studied SCADA system from a high level looking at components such as vulnerabilities with physical access to the SCADA system and countering it by applying a Role Based Access Control (RBAC) process. This work was more aligned with conceptual architectural design than as a pattern for secure implementation of SCADA/ICS systems, which would benefit security practitioners and system architects. Gobena et al. [10] devised a new wide area network communications mechanism for connecting SCADA and ICS services to ensure availability. However, the focus was not on the confidentiality or integrity of system messaging in any more detail. Wu et al. [11] focused on the implementation of controls to capture, analyse and report breaches of security with regards to SCADA and ICS based systems and services for the forensic investigation and ultimate recovery and prosecution of the threat actors where possible. The paper explains the different types of attack and proposes a detailed forensics process. Zhendong et al. [12] provided the most detailed approach towards an architectural implementation, however, as with previous research, this was not of a sufficient level to provide a practitioner with the necessary level of decomposition such that they could design and implement secure industrial systems and services. In sum, despite these works being focused on architectural reference and design, the majority were at too high a level for the security practitioner to use to implement a secure SCADA and ICS service without significant further decomposition.

This research is also motivated by industrial practices. Due to changes within Government Communications Headquarters (GCHQ)'s mission directive, whereby the scope of CLAS will be expanded to support the Critical National Infrastructure (CNI) with Information Assurance related matters, as well as the lack of advice for architects with regards to securing SCADA and ICS based systems, this research has been undertaken to provide a security architectural pattern to bridge the gap between CNI and IA, hence address SCADA/ICS systems risks.

1.3 The proposed security architectural pattern

However to date, very little documentation has been developed that provides an information assurance (IA) practitioners a holistic explanation of what the actual risks are and how to mitigate them. This paper presents a number of medium to high severity risks and proposes a security architectural pattern to address them. The architectural pattern is designed based on the Sherwood Applied Business Security Architecture (SABSA), which has been widely used to design business security frameworks [17, 18, 19, 20]. SABSA is selected because it is a robust and internationally recognised architecture methodology which focuses on the business requirements and develops from there. It has been used over other methodologies because of its business focus and ability to trace controls back to these requirements [8]. It helps removing the risk of developing technical architectures in isolation of what the business needs. In this paper, the architectural pattern is delivered based on the SABSA's top two layers, namely contextual and conceptual, which are responsible for understanding the business requirements and development of a concept architecture and strategy [8]. The concept architecture can then be taken forward by the IA practitioners and adjusted to satisfy the needs of their own organisations.

The remainder of the paper is structured as follows. Section 2 reviews the current architectural patterns for implementation of secure SCADA and ICS services. Section 3 presents a number of medium to high severity risks, whilst Section 4 presents the proposed security architectural pattern and Section 5 discusses the proposed security architectural pattern. Section 6 summarises the paper and lays the foundations for future work.

2 ICS Infrastructure

Traditional SCADA/ICS systems were composed of isolated networks without connection to others (e.g. corporate networks and the Internet) [13]. Most did not have the security risks we know today and subsequently were flat networks with very little control implemented. Based on CPNI documentation [14], Figure 1 summarises a typical SCADA and ICS network implementation today, which has evolved to become integrated with the corporate network as well as there having been the introduction of remote access and support capabilities with remote sites and third parties.

3 Risk Management

3.1 Threat Assessment

The Critical National Infrastructure (CNI) is subject to a number of threat sources, which are detailed below along with their representative scores regarding the threat level of them

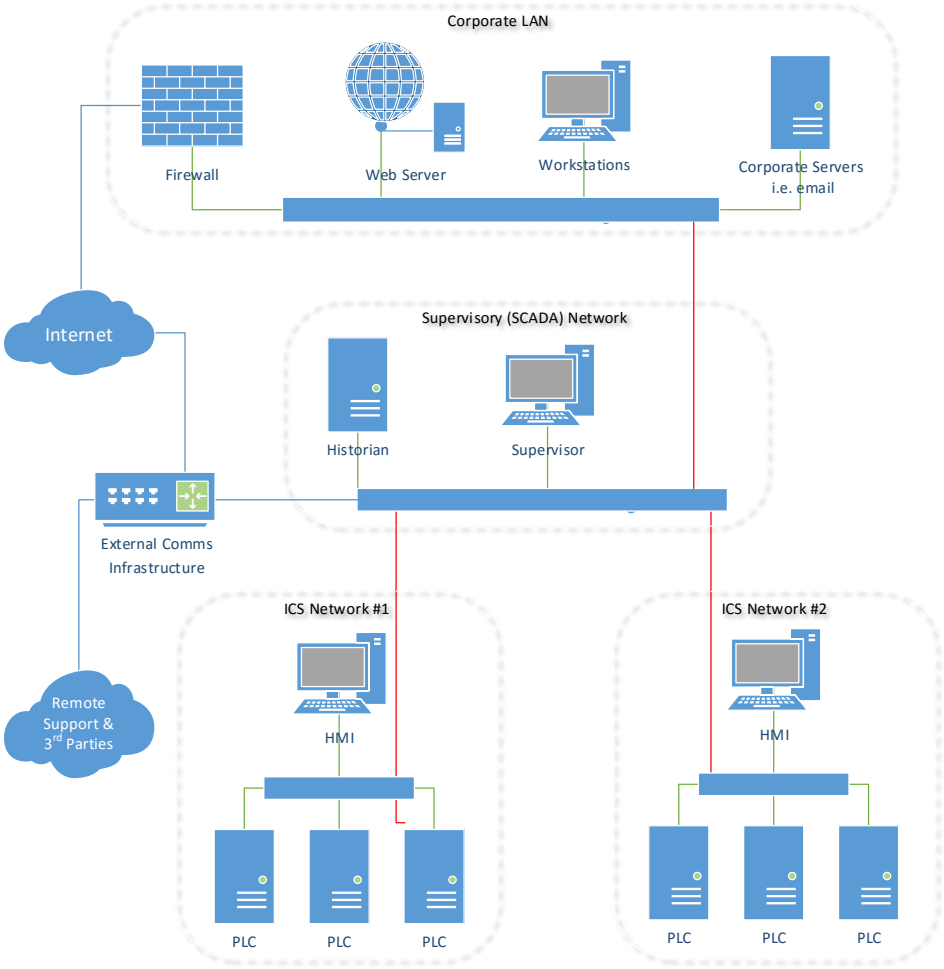

Figure 1 Typical SCADA and ICS deployment today

attacking a CNI provider. Table 1 provides a typical overview of threats, not exhaustive. This is based on Communications-Electronics Security Group (CESG) Information Assurance Standard 1/2 [34] which is used for risk management within the UK public sector, including CNI providers. Other sources of threats exist in documents such as ISO27001, CRAMM (Central Computer and Telecommunications Agency Risk Analysis and Management Method) and Pilar. A more focused assessment should be undertaken against the readers' organisation to understand the difference of their own threat profile and accommodate changes to satisfy their needs.

Table 1 Threat assessment

Ref.	Threat Source	Capability	Rationale	Motivation	Rationale
TS1	Disaffected or dishonest employees	High	Knowledge of internal systems and processes	High	This type of threat source will have a high probability of wanting to cause some form of damage to an organisation
TS2	Foreign Intelligence Services (FIS)	High	Highly skilled and funded	Low	CNI does not normally contain sensitive information which would be of interest to FIS
TS3	State Sponsored	High	Highly skilled and funded	High	This has been seen previously (e.g. Stuxnet)
TS4	Amateur hackers	Low	Low skilled/experience	Medium- High	The most common attack vector is incorrectly configured Internet facing systems. Amateur hackers tend to run vulnerability scans across the Internet and toolsets are available for those with limited knowledge/skill
TS5	Malware writers	High	High skilled programmers	Low	Most malware does not focus on SCADA/ICS platforms
TS6	Terrorists	Medium	Terrorists have become skilled over the last few years in cyber warfare	High	The CNI is a low cost viable attack vector for terrorists wanting to cause disruption to the UK
TS7	Investigative journalists	Low	Low skill, usually engaging in an external resource for cyber-attacks	Low	No useful information is held on SCADA/ICS systems for this threat source
TS8	Commercial competitors (i.e. industrial espionage)	Medium	Skills and knowledge of the systems and processes	Low- Medium	Competitive pricing and costs within the industry can drive industrial espionage from competitors
TS9	Political pressure groups/ activists	Low	Low skill and defacement of websites	Low	More focused on website attacks. Less focused on political causes
TS10	Organised criminal groups	Low- Medium	Low-medium skill set for ICS/SCADA attack	Low	More focused on credit card style fraud, laundering etc.
TS11	Academia and research	High	Highly skilled. Developing cutting edge research.	Medium	Indirectly, academia and research groups communicate vulnerabilities, exploits etc. through publications and seminars

It is clear from the threat assessment that there are a number of highly capable threat sources, which could have a vested interested in causing significant impact to the UK's national infrastructure. The type and level of security controls that need to be put in place to minimise risk from them needs to provide a significant defence in depth capability.

3.2 Risk Assessment and Treatment

Table 2 provides a high level risk assessment and treatment plan of a typical SCADA and ICS implementation based on SCADA and ICS deployment in section 2. Threat sources have only been shown where their risk has been assessed as medium or higher. The treatment (control) are to be applied to the previously identified risks to reduce them to an acceptable level. This is based on a qualitative approach, following the international standards organisation (ISO) 27005:2011 methodology [33].

Table 2: Risk assessment and treatment plan

Ref	Risk	Threat Source(s)	Impact	Severity	Treatment (Control)	Residual Risk
R1	Unauthorised access to control systems via public networks	TS2, TS3, TS4, TS5, TS6, TS8	High	High	Perimeter Security (Firewall), Network and host based intrusion detection, prevention system (IDS/IPS), Protective monitoring service, Auditing policy	None
R2	Lack of network segregation to provide containment	TS1, TS2, TS3, TS4, TS5, TS6, TS8	High	High	Tiered architecture methodology Firewall control at the security domain edge Virtual LAN (VLAN) separation of traffic types / services	None
R3	Lack of network auditing/monitoring	TS1, TS2, TS3, TS4, TS5, TS6, TS8	High	High	Protective monitoring service auditing policy	None
R4	Lack of firmware & software patching	TS2, TS3, TS4, TS5, TS6, TS11	High	High	Vulnerability assessment, System patching management toolset patching policy	None
R5	Lack of security awareness with respect to ICS/SCADA security	TS1, TS2, TS3, TS4, TS6, TS8	Medium	Medium	Security training and staff awareness programme induction policy, Security policy (wrt training and awareness)	None
R6	Lack of segmentation in the corporate network	TS1, TS2, TS3, TS4, TS5, TS6, TS8	Medium	Medium	Introduce security domains None, Tiered architecture	None

Table 2: (continued)

Ref	Risk	Threat Source(s)	Impact	Severity	Treatment (Control)	Residual Risk
R7	Lack of web application inspection for SCADA/ICS control	TS2, TS3, TS4, TS5, TS6, TS8	Medium	Medium	Layer 7 Web Application Firewall (WAF) Protective monitoring service	None
R8	Plain text data and commands being sent from the supervisor to control network	TS2, TS3, TS6	Medium	Medium	Virtual LAN (VLAN) segregation, Switch hardening to monitor and protect against CAM table flooding and VLAN hopping	Data will remain unencrypted if a secure communications protocol is unavailable
R9	Lack of regular vulnerability assessment	TS2, TS3, TS4, TS5, TS6	Medium	Medium	Vulnerability management software, Patch management service (including reporting)	None
R10	Lack of industry/sector threat intelligence	TS2, TS3, TS6	Medium	Medium	Sign up to industry WARP service or vulnerability advisory service4	None
R11	Compromise of corporate LAN will allow threat actor access to ICS/SCADA networks	TS2, TS3, TS4, TS5, TS6, TS8	High	High	Network segmentation - firewalls, Network intrusion detection or prevention system (NIDS/NIPS)	None
R12	The SCADA/ICS network external communications infrastructure introduces a bypass around the edge firewall	TS2, TS3, TS4, TS5, TS6, TS8	High	High	Perimeter security, Tiered Architecture, Security Policy	Residual risk if communications are over unsecure protocols and/or internal service does not authenticate connections

Table 2: (continued)

Ref	Risk	Threat Source(s)	Impact	Severity	Treatment (Control)	Residual Risk
R13	Remote support and third party access is via an uncontrolled gateway	TS2, TS3, TS4, TS5, TS6, TS8	High	High	Tiered Architecture, Network intrusion detection or prevention system (NIDS/NIPS), Protective Monitoring, RBAC, 3rd party security policy, 3rd Party code of connections (CoCo)	None

4 The Framework - Architectural Pattern

As mentioned above, the architectural pattern is delivered based on the SABSA security architecture framework's top two layers, namely, contextual and conceptual, which are responsible for understanding the business requirements and development of a concept architecture and strategy. The concept architecture can then be taken forward by the IA practitioner and made more relevant to his or her organisation and constraints. The pattern is delivered by starting with business requirements engineering, defining architectural principles for the design and finally developing the conceptual design itself with detailed information on the technical, governance and assurance controls implemented. The pattern also provides advice and guidance at managing legacy installations.

4.1 The Focus of Contextual & Conceptual Layers in SABSA

The contextual layer of the SABSA framework is concerned with identification of the business requirements (BR) and the development of security focused business drivers (BD), which will support the business requirements and drive the security architecture. Business Requirements (BRs) are obtained from the stakeholders and will be in the language of business. They will not specifically be security focused and nor will they be in the language a security professional may be familiar with. Business Drivers (BDs) are defined in the language of security to deliver, support and enable one or more of the BRs. A typical example of this could be that the Chief Operating Officer (COO) is "concerned that the ICS network must be up and running 100% of the time, any down time will have a financial impact on the organisation". This is a business requirement (from the COO). A BD to support/enable this would be "The availability of the ICS network must be maintained at 100% service".

The conceptual layer of this framework is concerned with normalisation of the business drivers (BD) into attributes[1] and development of the conceptual design. Figure 2 illustrates this process in diagrammatic form.

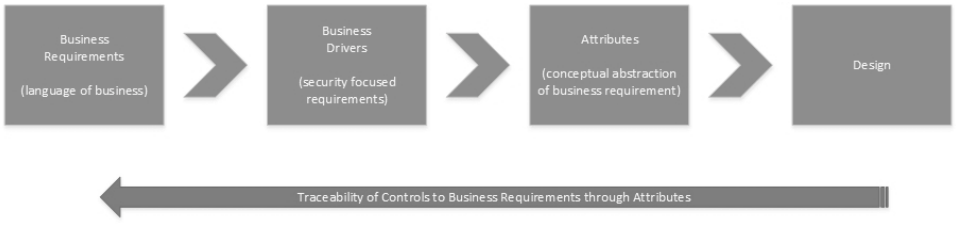

Figure 2 Architectural process

This pattern is designed to provide an overall holistic approach to delivering a secure architecture for SCADA and ICS based infrastructure. It is conceptual in nature, which means it is not intended to be a definitive architectural design for immediate implementation, but more a guidance design with services architected in line with best practice, up to date risk assessment as well as some degree of future proofing based on current and future trends ascertained from previous research.

4.2 Business Requirements

The business requirements will change depending on sector, regulatory demands, business and financial constraints etc. Table 3 details typical business requirements for a CNI provider as a generic starting point. SCADA and ICS systems work 24/7/365. Downtime refers to the business stopping, which can result in a financial impact as well as fines in some regulated industries, if the period of this time is above agreed limits. Therefore the main business focus is the availability of the SCADA and ICS systems.

Table 3 Business requirements

Ref.	Requirement
BR1	The service must maintain maximum up time and prevent control system disruption.
BR2	The service must be supportable remotely.
BR3	The SCADA system must be accessible by the corporate network for data exchange.
BR4	The service must be accessed by authorised staff only.
BR5	The service must be allowed to utilise connectivity across public networks, such as the Internet.
BR6	The service must have internal auditing and monitoring to identify system misuse or attack.
BR7	The service must deter threat sources identified as having a high likelihood of attack.
BR8	The service must deter internal threat actors (threat source TS1).
BR9	Prevent damage to the industrial systems and the ICS controls.
BR10	Prevent information leakage.

4.3 Business Drivers

Business requirements (BR) are high level requirements defined by the business stakeholders and as such can be complex, such as “deliver a secure ICT network”. So to be more specific, manageable, traceable and security focused business drivers (BD) are developed to support one or more BRs, thereby allowing complex requirements to be broken down and hence, managed more easily. Table 4 details the business drivers (BD) and what BRs they support.

4.4 Attribute Profiling

An attribute is defined [16] as a conceptual abstraction of a real business requirement (the goals, objectives, drivers and targets), which is modelled into a normalised language that articulates requirements and measures performance in a way that is instinctive to all stakeholders. Table 5 provides an attribute profile based on the BDs along with the standard definition from SABSA [16].

Table 4 Business drivers

Reference	Business Driver	Supporting BR
BD1	Provide accessibility of SCADA and ICS based systems remotely to authorised support staff.	BR2, BR4
BD2	Implement protective monitoring to audit key systems to capture information relating to system use/misuse, including at a minimum, action, username, source IP address, date and time.	BR6, BR7, BR8, BR9
BD3	Provide a mechanism for connecting the SCADA and ICS infrastructure to the corporate network for authorised support access.	BR3, BR4
BD4	Provide connectivity over cost effective public network channels, i.e. the Internet.	BR5
BD5	Provide connectivity from the corporate network for data exchange.	BR3
BD6	Identify and deter attacks from highly competent threat sources.	BR7, BR9, BR10
BD7	Implement architectural layering to provide containment controls and defence in depth to key assets.	BR7, BR9, BR10
BD8	Maintain availability of service to n%.	BR1
BD9	Minimise the risk of internal threat actors.	BR8

Table 5: Attribute profile

Requirement	Attribute	Definition
BD1	Authenticated	Every party claiming a unique identity (i.e. a claimant) should be subject to a procedure that verifies that the party is indeed the authentic owner of the claimed identity.
	Authorized	The system should allow only those actions that have been explicitly authorised.
	Access Controlled	Access to information and functions within the system should be controlled in accordance with the authorized privileges of the party requesting the access. Unauthorised access should be prevented
BD2	Monitored	The operational performance of the system should be continuously monitored to ensure that other attribute specifications are being met. Any deviations from acceptable limits should be notified to the systems management function.
	Auditable	The actions of all parties having authorised access to the system, and the complete chain of events and outcomes resulting from these actions should be recorded so that this history can be reviewed. The audit records should provide an appropriate level of detail, in accordance with business needs.
BD3	Interoperable	The system should interoperate with other similar systems, both immediately and in future as intersystem communication becomes increasingly a requirement.
	Access Controlled	Access to information and functions within the system should be controlled in accordance with the authorized privileges of the party requesting the access and unauthorised access should be prevented.
	Monitored	The operational performance of the system should be continuously monitored to ensure that other attribute specifications are being met and any deviations from acceptable limits should be notified to the systems management function.
BD4	Cost Effective	The design, acquisition, implementation, and operation of the system should be achieved at a cost that the business finds acceptable when judged against the benefits.
	Access Controlled	Access to information and functions within the system should be controlled in accordance with the authorized privileges of the party requesting the access and unauthorised access should be prevented.
	Monitored	The operational performance of the system should be continuously monitored to ensure that other attribute specifications are being met and any deviations from acceptable limits should be notified to the systems management function.
BD5	Interoperable	The system should interoperate with other similar systems, both immediately and in future as intersystem communication becomes increasingly a requirement.
	Access Controlled	Access to information and functions within the system should be controlled in accordance with the authorized privileges of the party requesting the access and unauthorised access should be prevented.
BD6	Detectable	Important events must be detected and reported.

Table 5: (continued)

Requirement	Attribute	Definition
	Monitored	The operational performance of the system should be continuously monitored to ensure that other attribute specifications are being met and any deviations from acceptable limits should be notified to the systems management function.
	Auditable	The actions of all parties having authorised access to the system, and the complete chain of events and outcomes resulting from these actions should be recorded so that this history can be reviewed. The audit records should provide an appropriate level of detail, in accordance with business needs.
	Access Controlled	Access to information and functions within the system should be controlled in accordance with the authorized privileges of the party requesting the access and unauthorised access should be prevented.
BD7	Architecturally Open	The system architecture should, wherever possible, not be locked into specific vendor interface standards and should allow flexibility in the choice of vendors and products, both initially and in the future.
BD8	Available	The information and services provided by the system should be available according to the requirements specified in the service- level agreement (SLA).
BD9	Detectable	Important events must be detected and reported.
	Monitored	The operational performance of the system should be continuously monitored to ensure that other attribute specifications are being met and any deviations from acceptable limits should be notified to the systems management function.
	Auditable	The actions of all parties having authorised access to the system, and the complete chain of events and outcomes resulting from these actions should be recorded so that this history can be reviewed. The audit records should provide an appropriate level of detail, in accordance with business needs.
	Access Controlled	Access to information and functions within the system should be controlled in accordance with the authorized privileges of the party requesting the access and unauthorised access should be prevented.

4.5 Design

The design phase is split between architectural principles, which define the underlying general rules and guidelines for the design, and the design itself.

4.5.1 Architectural principles

There are two key architectural principles to ensure the service is delivered against the business requirements, which are tiered architecture and the defence-in-depth model.

A tiered architecture allows for types of services (i.e. web/application services which present front end applications to users) to be collectively located within logical or physical domains where a security policy can be applied. A three-tiered architecture is typical of an infrastructure whereby end users and third parties will access the network through an access layer. This will be responsible for securing the user connectivity to the network either directly, i.e. switch port security, or indirectly, i.e. over remote access or virtual private networks (VPN). The presentation layer is responsible for locating the application services, user authentication to the applications, applying role based access control (RBAC), providing authorised views of data as well as auditing user activity within the application(s). The data layer is located in the heart of the network and connectivity is restricted to the authorised applications that need to access the database or data repository. Communication in this layer is usually restricted to application traffic using database commands, such as SQL.

Each layer is segregated from the others via firewalls, which are configured to allow only approved protocols and services through as strictly as possible. Figure 3 below shows a diagrammatic representation of a three-tiered architecture model.

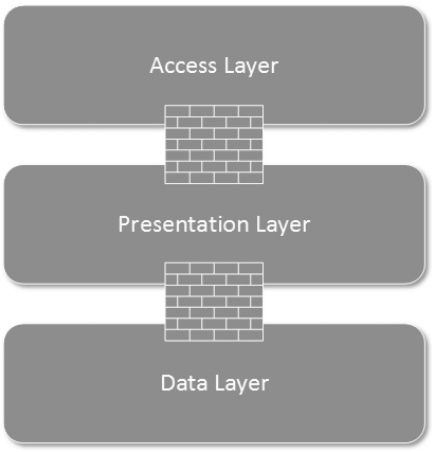

Figure 3 Tiered architecture model

The second is to deliver defence in depth [16] by layering security controls so as to reduce the risk to the assets being protected. As can be seen in Figure 4, by applying multiple controls "on top of" the information asset (in this case the SCADA and ICS configuration and management data) the architect introduces further barriers, which a threat actor has to

overcome. For the more competent threat actors this will slow them down within the time it takes to get through some of the controls, the protective monitoring service should have alerted someone to the attack, which will allow further action to be taken (such as dropping the threat actors connection).

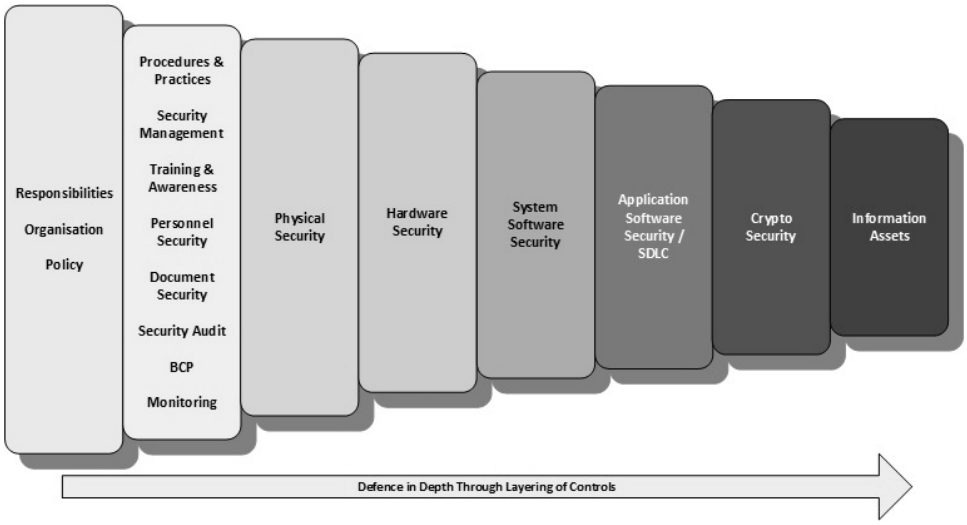

Figure 4 Defence in depth model

Defence in depth ensures there is no single point of failure from threats to assets by providing differing barriers (controls) in a layered approach. By applying the industry standard 80/20 rule (80% effectiveness of a control) to each control, you decrease the likelihood of a compromise exponentially as another control is layered on, as can be seen in Figure 5 below.

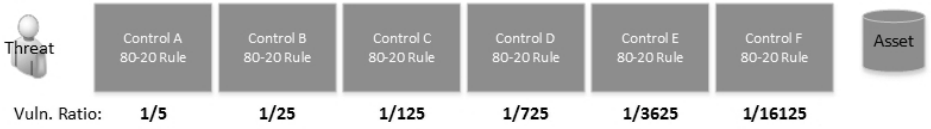

Figure 5 Defence in depth 80/20 rule

4.5.2 Conceptual design

In line with the business drivers, risk assessment and architectural principles above, Figure 6 describes the conceptual target architecture for delivering SCADA and ICS based services in a risk managed way. SABSA attributes have been added where relevant to the services to ensure appropriate controls are included during any revision of the design by the reader.

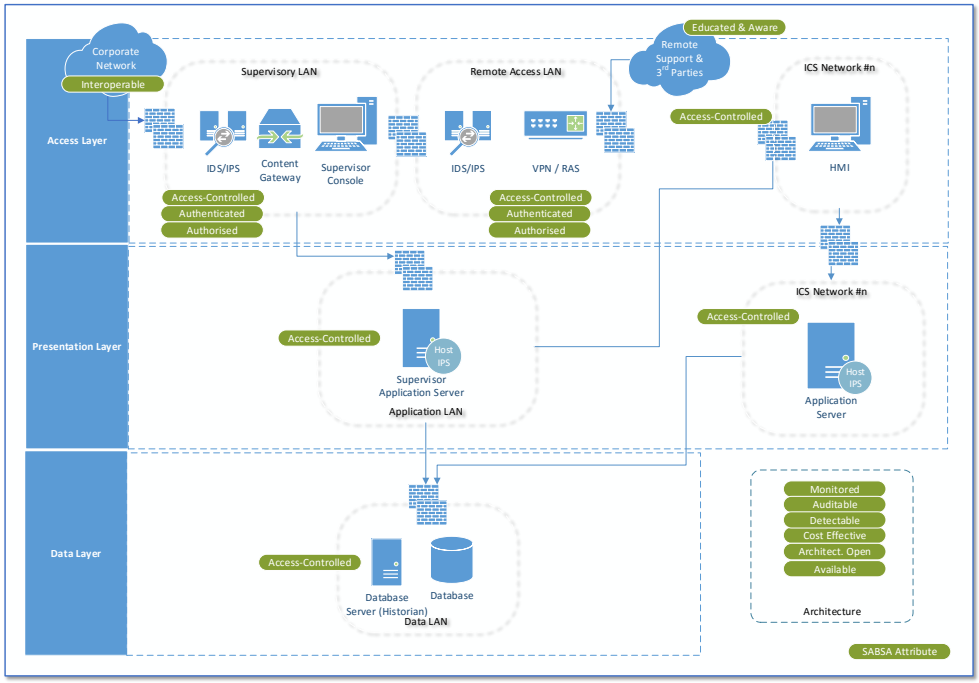

Figure 6 Target architecture

4.6 Components of the Architectural Pattern

This section provides more details about the control components within the target architecture. By applying the layering architectural principle, the three core components of the overall solution are split up into their own security domains and placed neatly in their representative layers, as follows.

4.6.1 Access layer

Access layer provides the first line of defence with connectivity to and from the "corporate network" as well as remote systems and support along with third party support,

- Data exchange between the corporate network and the SCADA/ICS network systems should be inspected for data schema validation and content inspection to ensure malicious packets are not injected into the SCADA/ICS network from the corporate network.
- Third party support should be configured to allow only the minimum system connectivity and access required as defined in a corporate third party security policy.
- Intrusion detection/prevention services monitor network communications from lower trust networks, such as the corporate network and remote/third party access networks.
- Remote access is managed through a dedicated RAS/VPN service, which, depending on make/model, can be configured to provide network access control (NAC) capability

to ensure remote endpoints meet a minimum level of technical security (i.e. security patches are up to date, AV signature definition is within acceptable delta etc.).

4.6.2 Presentation layer

Presentation layer delivers the application functionality and formats the information for further processing or display,

- RBAC configured within the applications to ensure users meet the principle of "least privilege" for their role(s).
- Segregation of security domains is achieved through layer 3 stateful firewalls.
- Application servers should have a host based IPS software agent installed to minimise risk to the host and application through attacks such as buffer overflows or malicious commands (i.e. SQL injection).

4.6.3 Data layer

Data Layer provides security for the backend databases and repositories,

- Segregation of security domains is achieved through layer 3 stateful firewalls.
- Consideration should be given to encrypting sensitive databases.
- Data read/write should only be possible from authorised accounts associated with the SCADA and ICS application(s).

Table 6 provides a list of the component security controls from the target architecture to form the basis of a bill of materials (BoM).

4.7 Traceability

A good architecture will start with the business requirements (BR), derive security focused business drivers (BDs) to support these and develop the necessary design to support the BDs. According to Palmer [28], "traceability provides support in understanding the relationships that across architectural requirements, design and implementation". Table 7 shows traceability mapping among business drivers, attributes and controls.

Table 6 Component list

Component	Purpose	Location
Network IDS/IPS	Analyse network packets for malicious content/activity.	Access layer
Firewalls	Segregated security domains and provide containment. Restrict traffic to approved protocols and source/destination addresses.	All layers
	Web Application Firewalls (WAF) provide layer 7 inspection of application traffic and can prevent malicious communications such as SQL injection.	Presentation layer
SIEM	Provide analysis of logged events from monitored endpoints to identify breaches (or suspected breach) in security policy.	All layers
RAS / VPN	Provide controlled remote access to the environment, enforcing security policy on remote users in the form of NAC as well as auditing and RBAC.	Access layer
Content Gateway	Provide schema and data validation checks on exported (and imported) data to (and from) the corporate network. For sensitive data, it would be advised also to implement data loss prevention (DLP) technology on the gateway to restrict exfiltration of data which should not leave the environment.	Access layer
Host IPS	Analyse OS and application processes to prevent attacks such as buffer overflows or malicious code injection.	Presentation layer
System Hardening	Best practice guidance to secure devices, OS and applications to reduce security footprint.	All layers
RBAC	Provide role based access control to staff to enforce minimum privilege levels for their role.	All layers
Anti-malware (not shown in diagram)	Installed on all systems where files can be exchanged and/or media (CD/DVD/USB keys etc.) can be installed.	All layers

Table 7 Architecture traceability to BDs

Business Driver	Attribute(s)	Control(s)
BD1	Authenticated, Authorised, Access-Controlled	Firewall, RAS / VPN
BD2	Monitored, Auditable	Protective Monitoring / SIEM, System Hardening
BD3	Interoperable, Access Controlled, Monitored	Firewall, Network IDS/IPS, Protective Monitoring / SIEM
BD4	Cost Effective, Access Controlled, Monitored	RAS / VPN, Network IDS/IPS
BD5	Interoperable, Access Controlled	Content Gateway, Firewalls
BD6	Detectable, Monitored, Auditable, Access-Controlled	Network IDS/IPS, Host IPS, System Hardening, Protective Monitoring / SIEM, Firewalls, RBAC
BD7	Architecturally Open	Firewalls
BD8	Available	All controls working to form defence in depth
BD9	Detectable, Monitored, Auditable, Access-Controlled	Network IDS/IPS, Host IPS, System Hardening, Protective Monitoring / SIEM, Firewalls. RBAC

5 Discussion

This pattern has achieved what it set out to do in a structured manner in that it has, firstly, identified current risks with SCADA and ICS systems, it then derived a typical set of business requirements for using industrial control technology, through a globally recognised security architecture framework, SABSA. For this research, a conceptual target architecture was developed, which can provide the basis for organisations to build their own target architecture. As the pattern is based on the principle of a tiered architecture, extensibility is made easier by introducing components into the correct tier and managing connectivity between tiers through the corresponding security controls.

The architectural pattern can be used to develop a future state architecture to drive the legacy platform towards through business change. Rather than the SCADA and ICS systems themselves, this pattern focuses on architecture of the infrastructure they operate within. SCADA and ICS systems connected directly by public connectivity are still common today and they allow for low capability threat actors to gain access. Simple "best practice" will reduce the overall risk and remove the low to medium capability threat actors from the equation. With the premise that no security is 100%, preventing the high capability threat actors is not possible. By following the defence in depth principle, the IA practitioner can slow their activities down through the barriers (controls) and with a good level of system auditing and anomaly detection within the protective monitoring service, the security team can be alerted in real time to any suspect or actual incident, thereby being able to take any action deemed necessary in a timely manner.

6 Conclusion and Future Work

SCADA and ICS security have attracted people's attention and there have been plenty of studies covering many aspects of these systems. Although a lot of information exists in various forms and formats on designing secure industrial control systems and networks, very little documentation has been developed to document a holistic view of SCADA/ICS system risks and to guide IA practitioners on how to mitigate these risks. This paper brings all that information together and providing a generic architectural pattern and holistic end to end view of the requirements, risks assessments and mitigations.

We have identified current risks with SCADA and ICS systems and proposes a security architectural pattern to address them. The newly developed architectural pattern is based on two layers of the SABSA framework, contextual and conceptual, which are responsible for understanding the business requirements and development of a concept architecture and strategy. The use of the SABSA framework allows the organisations to focus on their business and trace controls back to these requirements, removing the risk of developing technical architectures in isolation of the business needs. The deliverables include holistic sets of ICS/SCADA threat sources, risk assessment and treatment controls, typical sets of business requirements, business drivers, attributes and architectural design.

Extant research has provided rich security risk management and control methods. However, it has not clearly distinguished those that are suitable for SCADA/ICS. This research has addressed this issue by deriving holistic sets of risk management and architectural design requirements for SCADA/ICS. In addition, this research is motivated by industrial needs. The integration of industrial practices allows the framework to be more practical and suitable to guide IA practitioners in real practice.

A initial testing of the pattern has been shown through the risk assessment and risk treatment plan with the identified risk mitigation controls in the conceptual design. Future work should conduct more explicit testing such as the pattern implementation as part of an architectural engagement with a CNI service provider or in a virtualised environment subjecting to penetration testing.

References

[1] Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, Symantec Corp., Security Response 5 (2011).

[2] SANS Institute (2013). SANS SCADA and Process Control Security Survey. SANS Institute. Available from: http://www.sans.org/reading-room/analysts_program/sans_survey_scada_2013.pdf [Accessed 27/03/2014].

[3] Alcaraz, Cristina, Gerardo Fernandez, and Fernando Carvajal. "Security aspects of SCADA and DCS environments." Critical Infrastructure Protection. Springer Berlin Heidelberg, 2012. 120-149.

[4] International Electrotechnical Commission, Industrial Communication Networks - Network and System Security - Part 1-1: Terminology, Concepts and Models, IEC/TS 62443- 1-1 ed1.0, Geneva, Switzerland, 2009.

[5] Stouffer, K., Falco, J., Scarfone, K.*Guide to industrial control systems (ICS) security*. NIST special publication, 800-82, 2011.

[6] CPNI. PROCESS CONTROL AND SCADA SECURITY GUIDE 2. IMPLEMENT SECURE ARCHITECTURE. In Good Practice Guide, 2008.

[7] Technical Support Working Group, Securing Your SCADA and Industrial Control Systems, Department of Defense, Washington, DC, 2005.

[8] Sherwood, J. et al (n.d). Sherwood Applied Business Security Architecture. [WWW] SABSA Institute. Available from: http://www.sabsa.org. [Accessed 19/01/2014]

[9] Fernandez, E.B. et al. (2010) Designing Secure SCADA Systems Using Security Patterns. Proceedings of the 43rd Hawaii International Conference on System Sciences 2010. USA: IEEE.

[10] Gobena, Y. et al. (2011) Practical Architecture Considerations for Smart Grid WAN Network. 2011. USA: IEEE.

[11] Wu, T. et al. (2013) Towards a Layered Architectural View for Security Analysis in SCADA Systems. Nov 2012. Austria: AIT.

[12] Zhendong, M. et al. (2012) Towards a Layered Architectural View for Security Analysis in SCADA Systems. Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research 2013. UK: BCS.

[13] Macaulay, Tyson, and Bryan L. Singer. Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press, 2011.

[14] CPNI (2011). Configuring & Managing Remote Access for Industrial Control Systems. CPNI. Available from: http://www.cpni.gov.uk/documents/publications/2011/2011022-remote_access_for_ics_gpg.pdf [Accessed 24/05/2014]

[15] Wood, A. (2014). It's all about the attributes. Securing The Enterprise Weblog [Online] 10th April 2014. Available from: http://securingtheenterprise.com [Accessed 10/04/2014]

[16] Sherwood, J. et al (n.d). Sherwood Applied Business Security Architecture. SABSA Institute. Available from: http://www.sabsa.org. [Accessed 19/01/2014]

[17] Burkett, Jason S. "Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSAÂ®." Information Security Journal: A Global Perspective 21.1 (2012): 47-54.

[18] Coetzee, Marijke. "Towards a Holistic Information Security Governance Framework for SOA." Availability, Reliability and Security (ARES), 2012 Seventh International Conference on. IEEE, 2012.

[19] Alemu, Meskerem, and Abrehet Mohammed Omer. "Cloud Computing Security Framework for Banking Industry." HiLCoE Journal of Computer Science and Technology (2014): 78.

[20] Van den Bosch, S. F. "Designing Secure Enterprise Architectures A comprehensive approach: framework, method, and modelling language." (2014).

[21] Nicholson, Andrew, et al. "SCADA security in the light of Cyber-Warfare." Computers & Security 31.4 (2012): 418-436.

[22] Knowles, William, et al. "A survey of cyber security management in industrial control systems." International Journal of Critical Infrastructure Protection 9 (2015): 52-80.

[23] Ying He, Leandros Maglaras, Helge janicke, and Kevin Jones. An Indusrtial Control Systems Incident Response Framework.IEEE Conference on Communications and Network Security (CNS 2015). Florence, Italy, 2015

[24] Ying He, and Helge janicke. Towards Agile Industrial Control Systems Incident Response. 3rd International Symposium for ICS & SCADA Cyber Security Research. Ingolstadt, Germany, 2015

[25] Lopez Jr, Juan, et al. Using Attack Trees to Assess Security Controls for Supervisory Control and Data Acquisition Systems (SCADA). Proceedings of the 7th International Conference on Information Warfare and Security. Academic Conferences Limited, 2012.

[26] Xie, Feng, Tianbo Lu, Xiaobo Guo, Jingli Liu, Yong Peng, and Yang Gao. Security analysis on cyber-physical system using attack tree. In Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on, pp. 429-432. IEEE, 2013.

[27] Kordy, Barbara, Ludovic Pietre-Cambacedes, and Patrick Schweitzer. DAG-based attack and defense modeling: Don't miss the forest for the attack trees. Computer science review 13 (2014): 1-38.

[28] Palmer JD, Traceability RT, Dorfman M. Software Requirements Engineering. IEEE Computer Society, Washington, DC. 1997.

[29] Genge B, Graur F, Haller P. Experimental assessment of network design approaches for protecting industrial control systems. International Journal of Critical Infrastructure Protection. 2015 Dec 31;11:24-38.

[30] Morris T, Srivastava A, Reaves B, Gao W, Pavurapu K, Reddi R. A control system testbed to validate critical infrastructure protection concepts. International Journal of Critical Infrastructure Protection. 2011 Aug 31;4(2):88-103.

[31] Di Sarno C, Garofalo A, Matteucci I, Vallini M. A novel security information and event management system for enhancing cyber security in a hydroelectric dam. International Journal of Critical Infrastructure Protection. 2016 Jun 30;13:39-51.

[32] Alcaraz C, Zeadally S. Critical infrastructure protection: requirements and challenges for the 21st century. International journal of critical infrastructure protection. 2015 Jan 31;8:53-66.

[33] ISO I, Std IE. ISO 27005: 2011. Information technology - Security techniques - Information security risk management. ISO. 2011.

[34] National Technical Authority for Information Assurance. HMG IA Standard Numbers 1 & 2 Information Risk Management. Cabinet Office and CESG. April 2012.